アルゴリズム論特論 （塩田）

2009 年 7 月 9 日の課題

課題 次の離散対数を計算せよ。

(1) 法 1006003, 底 2 に対する 3 の離散対数

(2) 法 21111991, 底 3 に対する 5 の離散対数

(3) 法 221228081, 底 24 に対する 7 の離散対数

提出期限：7 月 23 日（木） （512 号室ポストまで）

サンプルプログラム

`http://lupus.is.kochi-u.ac.jp/~shiota/mc09/` 配下に以下のプログラムがある。

- 関数定義部 （ 前回と同じ ）
  `crypto.py`
- 単純検索による離散対数計算プログラム
  `DLP.py`
- 離散対数のデモプログラム
  `DL.py`
- Diffie-Hellman 鍵交換システムのデモプログラム
  `DH.py`